人工智能在网络安全防御中的应用

何少雄[1]，刘志滨[2]，谢之越[3]

[1]东北财经大学管理科学与工程学院 辽宁大连
[2]齐齐哈尔大学计算机与控制工程学院 黑龙江齐齐哈尔
[3]福州大学计算机与大数据学院 福建福州

【摘要】人工智能技术在各行各业中的应用价值较为突出，不仅可以便捷各项操作行为，还有助于满足预期的管理要求。在网络安全防御管理中，越来越多技术人员融入人工智能技术快速的应对系统中的安全隐患，减少安全问题的发生，降低网络安全工作成本，减轻网络安全工作人员换的工作量，满足网络安全运行的要求以及标准，通过实施人工智能网络安全防御系统将能够提高检测和响应速度，并更积极地预测和处理新出现的威胁。凸显人工智能技术本身的利用优势。

【关键词】人工智能；网络安全；防御措施；安全检测

Application of artificial intelligence in network security defense

Shaoxiong He[1], Zhibin Liu[2], Zhiyue Xie[3]

[1]School of Management Science and Engineering, Dongbei University of Finance and Economics, Dalian Liaoning Province, China
[2]College of Computer and Control Engineering, Qiqihar University, Qiqihar, Heilongjiang
[3]College of Computer and Big Data, Fuzhou University, Fuzhou, China

【**Abstract**】The application value of artificial intelligence technology is more prominent in all walks of life. It can not only facilitate various operations, but also help to meet the expected management requirements. In network security defense management, more and more technical personnel integrate artificial intelligence technology to quickly cope with the security risks in the system, reduce the occurrence of security problems, reduce the cost of network security work, reduce the workload of network security staff, meet the requirements and standards of network security operation, Through the implementation of AI cybersecurity defense systems will be able to improve detection and response speed, and more actively anticipate and deal with emerging threats. Highlight the advantages of artificial intelligence technology itself.

【**Keywords**】Artificial intelligence; Network security; Defensive measures; Safety inspection

1 引言

随着人工智能(AI)在社会中的日益普及，也进入了网络安全领域。人工智能可以在许多方面帮助改善网络安全，包括自动检测和响应威胁，提高网络效率，并帮助识别漏洞。计算机在人们日常学习和生活中的应用功能更加多样化，已成为人们生活和工作的重要工具。随着我国网络技术的高速发展，网络本身的开放性也越来越明显。安全问题更加多样化。要达到良好的安全防护效果，既要充分发挥人工智能技术本身的优势，做好网络运行过程的全面维护，也需要整合创新的技术解决方案，使计算机网络运行具有较强的稳定性和安全性。总结丰富的工作经验，构建更加成熟的安全防御机制，促进我国网络技术产业的可持续发展。

2 人工智能融入网络安全防御中的作用

2.1 完善的学习推理能力

将人工智能技术本身融入网络安全防御的优势更加突出。首先，人工智能技术本身的推理能力可

以用来判断其他安全风险，满足多个方向的网络安全防御工作需求，减少各种安全问题的发生。在网络环境管理方面，要以先进的保护技术为主要支撑，利用人工智能技术本身的功能，有效协调各个控制模块，并根据推理能力推断出其他安全风险，从而解决过去的安全问题。改进防御中存在的问题，提高整体管理水平。在过去的网络安全防御过程中，由于技术手段的限制，对不安全信息的处理存在很多不确定性，也会出现一定的疏漏。因此，需要在实际工作中充分利用人工智能技术。根据自身优势，做好网防管理，配合人工智能技术本身的学习推理能力，有效管理和监督各种数据[1]。以某一数据作为推断其他安全系统的主要理由，及时发现其中的隐患，进一步保证数据本身的处理效率，维护我国当前网络环境的安全性，并突出利用人工智能技术本身的优势。

2.2 强大的模糊信息处理能力

当人工智能技术融入网络安全防御时，也可以充分利用人工智能技术的模糊信息处理能力，对不可预测的安全风险和突发事件的响应能力较强，对系统运行的影响降低[2]。在现代网络发展的过程中，在网络运行的过程中，开放性的特征更加突出，这将导致信息的类型逐渐增加，传播速度不断加快。再加上互联网通信和互联的功能，一些信息安全难以得到有效的确定，进而影响信息安全管理的有效性[3]。因此，在实际工作中，既需要利用人工智能技术本身的模糊信息处理能力对信息进行基本判断，消除各种不确定因素对网络安全管理的影响，也需要整合不同的网络安全管理资源。处理相应的信息。例如，在技术实施过程中，根据模糊信息处理收集的内容，总结丰富的工作经验，制定专门的安全管理模式，降低各种安全风险对网络系统运行的影响。全面强化整体安全管理效果，避免各种突发问题的发生。

2.3 网络防御协作能力较强

强大的网络防御协同能力也是人工智能技术融入网络安全防御的重要功能。伴随着我国网络技术的应用发展，应用功能越来越复杂，这也在一定程度上增加了出现问题的概率，并且在技术模型优化的过程中，逐渐朝着系统化的趋势发展，在此背景下，对网络安全防御能力提出了许多要求。因此，在实际工作中，要实现技术模式的创新发展，利用人工智能技术来完成当前的安全防御任务。在实际工作中，可以建立不同层次的智能管理系统，实现对各个环节的有效监督，进而贯穿各个环节。相互之间的配合和连接，构建完整的工作体系，全面保证网络安全防御的效果[4]。

2.4 工作防御的成本低

传统的网络安全系统在计算过程中消耗大量资源，安全效率也较低，使得整体网络安全防御成本较高，不利于相关部门实现经济效益和社会效益。使用人工智能技术应用于网络安全防御，可以有效避免传统防御方式的高成本。这是因为人工智能技术可以利用大量先进的算法来实现数据的精准开发，计算相关数据的精度，实现智能化安全管理。大大提高了各种资源的利用效率，实现了网络数据的优化配置。这有效降低了成本计算中软硬件系统的开发成本，为人工智能技术的深入推广奠定了坚实的基础[5]。

3 人工智能技术在网络安全防御中的具体应用

3.1 智能防火墙技术

将人工智能技术融入网络安全防御时，需要在原有技术解决方案的基础上不断创新和调整，再根据网络安全防御的要求和标准，对现有的管理体制进行创新，更符合现代网络的发展方向。例如，在实际工作中，可以将人工智能技术集成到防火墙中，达到良好的防护效果。防火墙属于隔离控制技术的范畴，它包括过滤技术和状态检测技术等。在使用人工智能技术的过程中，可以在网络层传输相应的数据包，使得防火墙的防护和控制更加准确。然后根据安全防护的要求，做好数据包地址的分析，逐条检查外部信息，减少安全风险的发生[6]。此外，人工智能技术还可以集成到状态监测中。需要构建不同的数据包，做好对各种安全风险的综合监管，有效维护网络环境本身的安全因素。

3.2 自动检测技术

保护企业网络的第一步是检测威胁。快速检测不可靠的数据将是理想的选择。它将保护网络免受永久性损坏。将人工智能与网络安全相结合是实时检测和响应威胁的最佳方式。人工智能检查整个系统的风险。与人类智能不同，网络人工智能能够及早发现风险，从而产生更快、更准确的安全警报，

从而提高网络安全专家的工作效率。

自动检测技术主要针对使用电子邮件进行科学防护，电子邮件已成为人们日常生活中的重要物品，虽然方便了每个工作行为，但在此过程中，人们会受到不同类型的垃圾邮件的影响，不仅会逐渐增加信息接收量，如果有安全保护意识不强。点击垃圾邮箱中的链接，很可能导致电脑被病毒入侵。因此，在实际工作中，有必要利用人工智能技术对现有的检测模式进行改进，避免对网络安全管理造成严重影响[7]。在系统应用过程中，可以对接收到的信息进行有效检测，然后快速分析是否含有病毒，并与病毒库数据进行相互比对，发现威胁因素应立即删除。这样可以引入各种繁琐的信息对安全管理的影响，为人们构建更加稳定的网络信息安全环境，提高人工智能技术本身的使用效果。

3.3 人工神经网络技术

人工神经网络技术在安全防御中的应用也比较重要，它可以达到立体的安全效果，人工神经网络技术本身的解析力很强，能够快速对各种不良信息进行分类和选择，也可以利用自身的学习能力和数据计算能力完成信息的存储和共享，充分发挥多元化优势，建立完善的安全防范体系，构建基于时间序列的预测模型快速识别计算机中的病毒，使安全防护工作更加准确，满足现代安全管理的要求。同时，用户还可以根据数据分析得到更准确的防御结果，了解计算机的基本运行情况，进而制定更科学的安全防护措施，让每台设备的运行都具有很强的安全系数，满足日常使用要求。

3.4 入侵风险预测

用于识别异常行为或活动模式的预测分析是人工智能在网络安全领域的主要应用之一。网络罪犯总是在寻找使用该系统的新方法。人工智能可以帮助在这些新威胁造成任何损害之前识别它们。人工智能系统有助于确定 IT 资产列表，并为所有设备、用户和应用程序提供具有不同访问权限的各种系统的完整准确列表。现在，考虑到资产库存和威胁暴露（如上所述），基于人工智能的系统可以预测它们最可能受到黑客攻击的方式和地点，使它们能够规划哪些资源最容易受到攻击。这种入侵风险预测将帮助组织做好准备，限制影响并打破攻击链。此外，可以开发和修改风险数据、政策和程序，以通过基于人工智能的分析提高网络弹性。

3.5 专家系统

专家系统是当前人工智能领域中应用较为成熟的技术，包含了推理功能和知识库等等，以专家知识为主要的基础进行模拟性的学习之后，再处理在网络安全防御中的各项问题，全面的提高整体的处理效果。在专家系统运用的过程中，比较依赖的是知识库本身的储量和专业度，为了提高整体的安全防护效果，可以融入先进的检测系统进行辅助性的利用，按照系统运行的要求，做好海量信息的深入性检测，之后再整合不同的安全特征行为，精准性的计算系统的参数规律，并且可以快速发现其中的异常规则，防护各种入侵行为，减少安全问题的发生。

4 结束语

将人工智能技术融入网络安全防御的优势比较突出。不仅可以灵活应对网络安全防御中的问题，还有助于实现安全技术模式的更新升级。人工智能可以成为打击网络犯罪的有力工具。通过自动化，人类安全分析师当前执行的任务可以减少误报的数量并加快检测和响应的过程。更重要的是要意识到与使用人工智能相关的潜在风险，并采取措施减轻风险，为人们使用网络创造良好的环境。因此，在实际工作中，需要加强对人工智能技术应用点的深入解读，更新现有技术方案，提升网络安全防御效果。

参考文献

[1] 刘元斌.人工智能及其在计算机网络技术中的实施策略浅谈[J].计算机产品与流通，2020(04)：148.

[2] 蓝方力.人工智能技术在网络安全防御中的应用价值研究[J].数字技术与应用,2020,38(10):186-188.

[3] 吴京京.人工智能技术在网络安全防御中的应用探析[J].计算机与网络,2017,43(14):60-61.

[4] 姜发健.人工智能技术在大数据网络安全防御中的应用[J].计算机产品与流通,2019(04):148-149.

[5] 秦利娟,张娴静.人工智能技术在网络安全防御中的应用研究[J].赤峰学院学报(自然科学版),2018,34(08):55-56.

[6] 马遥.基于大数据及人工智能技术的计算机网络安全防御系统设计[J].信息与电脑(理论版)，2020，32(04)：20

8-209.

[7] 于職.探究人工智能技术在网络空间安全防御中的应用[J].计算机产品与流通，2020(01)：146.

收稿日期：2022 年 8 月 18 日
出刊日期：2022 年 9 月 6 日
引用本文：何少雄，刘志滨，谢之越，人工智能在网络安全防御中的应用[J]. 国际计算机科学进展, 2022, 2(2) : 1-4.
DOI: 10.12208/j. aics.20220012

检索信息：RCCSE 权威核心学术期刊数据库、中国知网（CNKI Scholar）、万方数据 （WANFANG DATA）、Google Scholar 等数据库收录期刊